

Received & Inspected

DOCKET FILE COPY ORIGINAL

FEB 182015

FCC Mail Room

February 6, 2015

Honorable Thomas Wheeler Chairman Federal Communications Commission 445 12th Street Washington, DC 20554

Re: **ET Docket No. 14-143**

Dear Chairman Wheeler:

I am writing in response to your December 14, 2014 letter regarding mobile theft protection. I appreciate the opportunity to outline for you our thoughts on the issues you raised in your letter:

1. Making "lock/wipe/restore" functionality operational by default on all devices

U.S. Cellular is active in the support of smartphone theft deterrence via a diverse set of initiatives. U.S. Cellular encourages all of our OS or device partners to develop anti-theft capabilities, and in no way prohibits or restricts development of these capabilities through our requirements. Today, over 96% of our smartphone customer base is covered by solutions provided at no cost by our device or OS partners. We would welcome any efforts by our device or OS partners to have such functionality operational by default.

2. Protecting unique identifiers from alteration

As a non-national carrier, it is difficult for us acting alone to drive the development of new unique identifiers; however, we stand ready to adopt any industry-wide changes to device identifiers that are adopted by standards bodies and implemented by our OEMs.

3. Improving the timeliness, accuracy and availability of data about smartphone theft for use by law enforcement... and ... 4. Ensuring employees in your retail and authorized reseller affiliates understand the importance of their role in preventing mobile device theft by checking the appropriate database to ensure that every device they initialize for service has not been reported list or stolen.

We have recently completed the deployment of a new billing and operational support system that has given us the ability to deploy an operational database for internal use to combat theft of our devices by creating an internal blacklist. If a customer calls and reports their device lost or stolen, the Associate will process a lost/stolen device request. When processing this request, it will automatically add the lost/stolen device to a system blacklist

Honorable Thomas Wheeler Page 2
February 6, 2015

which prevents the device from being activated on our network by another customer. If the lost or stolen device is abandoned and left with the Associate, they will check for a corresponding Device Protection claim. If it does have a claim against it, our Device insurance provider is contacted. If the recovered property does not have a corresponding Device Protection Claim, the associate will review the account to identify a police report number (if applicable) and notify the appropriate police agency in the event the agency needs the recovered device as evidence.

In addition, now that we have our new system operational, I have also instructed my team to integrate our internal database with the industry GSMA database so that we can begin sharing information via that platform as soon as possible. We will notify you when that integration has been completed.

We also look forward to working with OEMs, the wireless industry and public safety agencies to evaluate and implement the recommendations of the TAC. In its initial comments in this docket filed last week, our trade association, CTIA, has raised a number of points relevant to implementation of the TAC recommendations, and we will continue to participate in CTIA's work with the TAC to achieve its goals. In addition, we also share the concerns raised by the Competitive Carriers Association in its comments about the ability of non-national carriers to drive multi-dimensional industry-wide solutions. That said, we remain very committed to working co-operatively with industry, public safety and the FCC to address the crucial challenge posed by mobile device theft.

Sincerely,